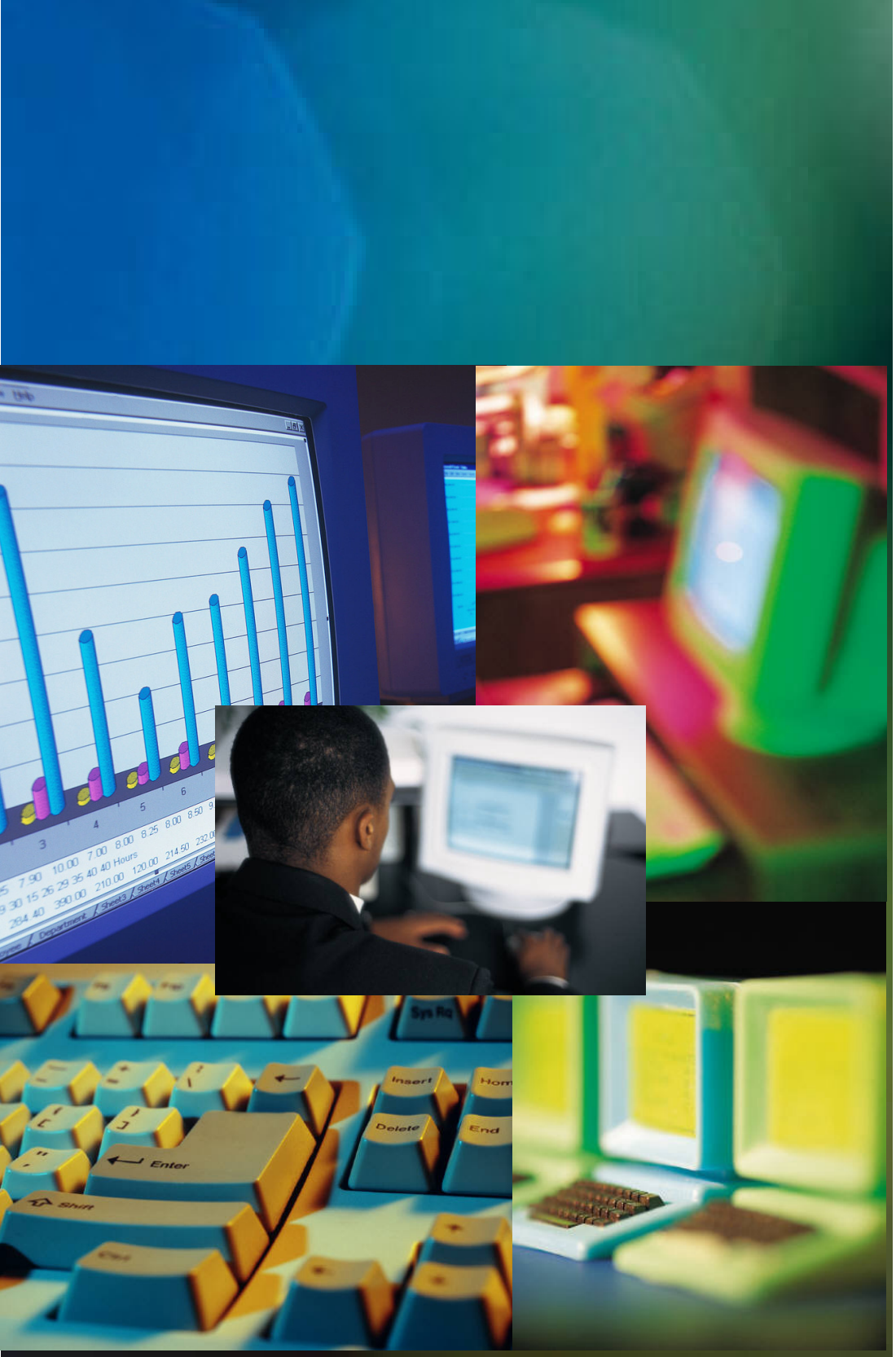

Homeless Management Information System Data and Technical Standards Notice

Frequently Asked Questions

July 2005

Prepared by
Abt Associates Inc.

List of Questions

List of Questions i

Frequently Asked Questions 1

1. Overview of HMIS Notice 1
- 1.1 Why did HUD create national data and technical standards for HMIS? 1
- 1.2 Who should participate in HMIS? 1
- 1.3 What are the requirements regarding data submission by providers to the local Continuum of Care? 2
- 1.4 What is HUD's expectation for implementing HMIS? 2
- 1.5 Does HUD expect that all HMIS data will be collected only from people who meet HUD's definition of homeless? 2

2. Implementing the HMIS Notice: Universal and Program-Specific Data Elements 3
- 2.1 What programs are required to collect the universal data elements? 3
- 2.2 What programs are required to collect the program-specific data elements? 3
- 2.3 Are the response categories associated with each data element required and can local service providers create additional response categories? 4
- 2.4 Is the Household Identification Number a unique number? 5
- 2.5 How is the Personal Identification Number (PIN) used? 5
- 2.6 What is the FIPS code in the "Program Identification Information" data element? 5
- 2.7 What is the CoC code in the "Program Identification Information" data element? 6
- 2.8 What is the facility code in the "Program Identification Information" data element? 6
- 2.9 What type of service should be recorded as "Temporary housing and other financial aid" in the Services Received program-specific data element (3.9)? 6
- 2.10 Should programs collect the detailed information in the Veteran's Information data element (optional data element 3.16) for each military service era? 6

3. Implementing the HMIS Notice: Privacy Standards 6
- 3.1 Can a HIPAA covered entity collect the required HMIS data elements and still be consistent with the HIPAA rule? 6
- 3.2 Do the HMIS privacy standards conflict with other federal laws regulating the collection and uses of personal information? 7
- 3.3 What happens if other federal, state, or local laws are found to be in conflict with the HMIS privacy or security standards? 8
- 3.4 For a basic community shelter (CHO) with no federal funding, who holds the shelter accountable for the misuse of client information collected for HMIS purposes? 8
- 3.5 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures required by law"? 8
- 3.6 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures to avert a serious threat to health or safety"? 9
- 3.7 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures about victims of abuse, neglect, or domestic violence"? 10

3.8 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures for law enforcement purposes"? 11
3.9 What is meant by client "consent" for all uses and disclosures specified in the HMIS privacy standards? 12
3.10 Can HUD provide sample privacy notices that are compliant with the HMIS standard? 12
3.11 Who is obligated to post the notice of privacy practices on a website? 13

4. Implementing the HMIS Notice: Technical Standards 13
4.1 Which of my computers and systems are affected by the new security standards? 13
4.2 Who is required to implement Public Key Infrastructure (PKI) or other similar means to restrict access to the HMIS? 14
4.3 What is the definition of a "public forum"? 14
4.4 Are PKI implementations difficult and costly? 14
4.5 Is PKI or encryption required for an HMIS using Citrix or Microsoft Terminal Services? 15
4.6 When the final notice refers to an "individual firewall" for a workstation, what does that mean? 15
4.7 Can a "wireless network" (or connection) comply with the HMIS security standards? 16
4.8 Is a firewall needed if we use Citrix to access our HMIS? 16

5. HMIS Data Standards and HUD's Annual Progress Reports 16
5.1 Was there an error in the "Cross-walk of HMIS and APR Response Categories for Destination" on page 45919 of the final notice? 16
5.2 How do the new ethnicity and race categories in the final notice correspond to the categories in the Annual Progress Report? 16

Appendix A: Baseline Model Privacy Notice for Homeless Organizations 18

Appendix B: Cross-walk of HMIS and APR Response Categories for Destination 30

Homeless Management Information Systems Data and Technical Standards Notice: Frequently Asked Questions

HUD published the Homeless Management Information System (HMIS) Data and Technical Standards Final Notice on July 30, 2004. The final notice describes the types of data that HUD-funded providers must collect from clients receiving homeless assistance services. The notice also presents privacy and system security standards for providers, Continuums of Care and all other entities that use or process HMIS data.

Since the release of the notice, HUD has received numerous questions about local implementation of the data and technical standards. This documents provides answers to some of the most frequently asked questions.

1. Overview of HMIS Notice

1.1 Why did HUD create national data and technical standards for HMIS?

HUD developed the HMIS national data standards for three important reasons.

- First, the data standards provide clear and precise meanings for the types of information collected by local homeless assistance providers and thus ensure that providers are collecting the same types of information consistently. The standards allow CoCs to analyze the characteristics of people experiencing homelessness in their community and compare the results with other communities, knowing that they are "comparing apples with apples," which is the only way to meaningfully understand the nature of homelessness.
- Second, the national standards will help further standardize reporting across federal programs and across other funders of programs for the homeless. Beginning with the first meetings to develop the national standards, HUD has been working with other federal agencies (e.g., the Department of Health and Human Services, the Veterans' Administration, and the Department of Education) to use HMIS as the primary tool for fulfilling program reporting requirements across agencies. In short, national data standards have the potential to greatly streamline reporting requirements and permit analysis of how programs are (or are not) working together to address homelessness.
- Finally, prior to the release of the HMIS standards, communities had not implemented uniform privacy and security provisions to adequately protect client confidentiality. The national standards include privacy and security requirements that are a significant improvement over past practices, set high baseline standards for all users of HMIS data, and provide important safeguards for personal information collected from all homeless clients.

1.2 Who should participate in HMIS?

The final notice states that recipients of HUD McKinney Vento Act program funds (Emergency Shelter Grants, Supportive Housing Program, Shelter Plus Care, and Section 8 SRO programs) are expected to

participate in a local HMIS. The Notice also indicates that Housing Opportunities for Persons with AIDS (HOPWA) funded programs that target homeless persons are also expected to participate.

In addition to these HUD-funded programs, HUD is encouraging participation by all other programs within a CoC that serve homeless persons, especially other federally-funded programs.

1.3 What are the requirements regarding data submission by providers to the local Continuum of Care?

Homeless assistance providers who participate in the local HMIS are required to submit HMIS data to the central server that is maintained by, or on behalf of the CoC's system administrator, at least once a year. With the exception of domestic violence agencies, the standard requires that all McKinney Vento-funded programs that assist homeless persons submit the universal data elements for each client served at least annually. In addition, HUD McKinney Vento programs that complete Annual Progress Reports (APRs) are required to submit program-specific data elements 3.1 through 3.11 (3.1 Income and Sources; 3.2 Non-Cash Benefits; 3.3 Physical Disability; 3.4 Developmental Disability; 3.5 HIV/AIDS; 3.6 Mental Health; 3.7 Substance Abuse; 3.8 Domestic Violence; 3.9 Services Received; 3.10 Destination; and 3.11 Reasons for Leaving) for each client served.

Given the unique circumstances of their clients, domestic violence shelters are not required to submit personal identifying client-level information to the CoC. Instead, domestic violence shelters may use a proxy, coded, encrypted, or hashed unique identifier—in lieu of personal identifying information—that is appended to the full service record of each client served and submitted to the central server at least once annually for purposes of de-duplication and data analysis. HUD is currently working with several privacy experts to (1) determine what personal information should be excluded from client records and (2) how to produce a hashed unique identifier that protects client confidentiality and also allows for accurate deduplication. Further guidance to domestic violence programs on these issues is forthcoming.

1.4 What is HUD's expectation for implementing HMIS?

The 2005 CoC SuperNOFA application requires that Continuums of Care describe their progress toward implementing an HMIS that is compliant with the final HMIS Notice. The 2005 application awards a maximum of 5 points for demonstrating progress on HMIS implementation, which includes a description of current and/or future strategies to implement the HMIS standards (e.g., participation, data elements, privacy, security) and the CoC's strategy to monitor and enforce compliance (see Form HUD 40076 CoC-J page 2).

1.5 Does HUD expect that all HMIS data will be collected only from people who meet HUD's definition of homeless?

HUD encourages all providers of homeless services to participate in HMIS. The experiences of communities with long-standing systems show that participation among the full-range of homeless service providers offers many benefits. For example, communities with broad participation are better able to use HMIS for comprehensive coordination and planning of homeless services than communities with participation from only a few providers.

Accordingly, HUD expects that all HUD-funded programs will provide data to HMIS and recognizes that participation from non-HUD funded providers—including providers that serve persons who do not meet HUD's definition of homelessness—is important. HUD-funded programs will be able to use HMIS data, including program entry/exit dates and prior residence information, to distinguish between clients who meet HUD's definition of homelessness and clients who use homeless services but do not meet this definition. HUD's definition of homelessness is found on the following website: http://www.hud.gov/offices/cpd/homeless/who.cfm

2. Implementing the HMIS Notice: Universal and Program-Specific Data Elements

2.1 What programs are required to collect the universal data elements?

All McKinney Vento funded homeless assistance providers are required to collect the universal data elements from all clients receiving homeless assistance services. The universal data elements include:

- 2.1 Name
- 2.2 Social Security Number
- 2.3 Date of Birth
- 2.4 Ethnicity and Race
- 2.5 Gender
- 2.6 Veteran Status
- 2.7 Disabling Condition
- 2.8 Residence Prior to Program Entry
- 2.9 Zip Code of Last Permanent Address

They also include several computer-generated elements that are not collected directly from the client and are assigned to each client record The computer-generated data elements include:

- 2.10 Program Entry Date
- 2.11 Program Exit Date
- 2.12 Unique Person Identification Number
- 2.13 Program Identification Number
- 2.14 Household Identification Number

The universal data elements are needed to understand the extent of homelessness, the characteristics of homeless clients, and the patterns of service use for the entire homeless population.

2.2 What programs are required to collect the program-specific data elements?

Most of the program-specific data elements are required for HUD McKinney Vento programs that are required to submit Annual Progress Reports. These programs are Shelter Plus Care, the Supportive Housing Program, Section 8 SRO Mod Rehab for the homeless, and HOPWA-funded homeless programs. The required data elements for programs that submit APRs include:

- 3.1 Income and Sources
- 3.2 Non-Cash Benefits
- 3.3 Physical Disability
- 3.4 Developmental Disability
- 3.5 HIV/AIDS
- 3.6 Mental Health
- 3.7 Substance Abuse
- 3.8 Domestic Violence
- 3.9 Services Received
- 3.10 Destination
- 3.11 Reasons for Leaving

Program-specific data elements 3.12 through 3.17 are optional. The optional program-specific data elements include:

- 3.12 Employment
- 3.13 Education
- 3.14 General Health Status
- 3.15 Pregnancy Status
- 3.16 Veteran's Information
- 3.17 Children's Education

These data elements have been recommended by a team of HMIS practitioners, federal agency representatives, and researchers, and they are based on best practices that are currently being implemented at the local level.

2.3 Are the response categories associated with each data element required and can local service providers create additional response categories?

All of the *response categories* for both the universal and program-specific data elements are required for programs that must collect this information. Service providers can create more detailed response categories as long as these categories can be aggregated to the categories presented in the HMIS standards. For example, a program that is required to collect the program-specific data elements may disaggregate the "Earned Income" response category in data element 3.1 (Income and Sources) into various types of earned income, such as earned income from full-time employment, from part-time employment, or from seasonal work. For reporting purposes, programs would collapse the three earned-income categories into the single response category (i.e. "Earned Income").

Service providers may also choose to include "Don't Know" or "Refused" response categories in data elements where these categories are not required by the HMIS standards. Providers that add these categories will need to decide how to handle this information for APR reporting purposes. For example, because the APR does not include "Don't Know" or "Refused" response categories, these responses categories should be treated as missing values and will not be reported on the APR. However, the APR should account for every person served during the operating year in question 2.

2.4 Is the Household Identification Number a unique number?

The Household Identification Number is used to identify whether a client is entering a program as a single or as part of a larger household. Based on the HMIS Notice, a household is a group of persons who together apply for homeless assistance services. The Household Identification Number is assigned to each client, and clients that are part of the same household for a particular program episode should be assigned a unique household identification number. These numbers should not be re-used within the program.

2.5 How is the Personal Identification Number (PIN) used?

The PIN is a unique identification code for each person served by a homeless assistance program. Where programs are sharing at least some data—e.g., personal identifying information—with other providers within a CoC, the PIN is unique across these HMIS-participating providers. Where there are no data shared across providers, the PIN will be unique only within a program.

The PIN can be used to de-duplicate client records. During the intake process, the intake worker enters basic information about the client (name, date of birth, etc.) and the HMIS searches the provider's system or community-wide network (depending on whether data are shared) to see if the client has been previously served by the program or by the larger network of programs. If a match is found, the HMIS retrieves the unique PIN and assigns the PIN to the current client record or appends the new data to the existing record. In this way, each client is associated with a single, unique code that is not based on personal identifying information and never changes. As such, the PIN becomes the primary key for producing a de-duplicated count. If a match is not found, the HMIS should produce a new unique PIN.

2.6 What is the FIPS code in the "Program Identification Information" data element?

The Program Identification Information data element is composed of 4 different codes: a 10-digit FIPS code, a Continuum of Care code, a facility code, and a program type code. The Federal Information Processing Standards (FIPS) Code is developed by the U.S. Census Bureau and is composed of a 2-digit state code, 3-digit county code, and 5-digit place code. The code gives communities the information needed to understand how their homeless service providers are geographically distributed across their community. This information is especially useful for comparing the location of homeless service providers with known concentrations of homeless persons. This comparison may reveal important gaps in the location of service providers compared to service need.

A FIPS code should be assigned to each service provider. It is not necessary to assign a FIPS code to administrative offices or other facilities that do not provide services to homeless persons.

To find the 10-digit FIPS code: (1) go to website http://geonames.usgs.gov/fips55.html; (2) click on "Search the FIPS55 Data Base;" (3) click on state from the "State Number Code" pull down menu (this also tells you 2-digit state code); (4) type town or city name in "FIPS 55 Feature Name" box; and (5) click on "Send Query."

2.7 What is the CoC code in the "Program Identification Information" data element?

The Program Identification Information data element is composed of 4 different codes: a 10-digit FIPS code, a Continuum of Care code, a facility code, and a program type code. The CoC code identifies each Continuum of Care throughout the country and is assigned by HUD. In the past, the CoC codes changed from year to year. HUD has now standardized these codes so that HMIS developers and administrators can "hard-code" them into their software. A full list of CoC codes are available on both the hmis.info website (http://www.hmis.info/ta_resources_data.asp?topic_id=10) and on HUD's Community Planning and Development SuperNOFA web page (http://www.hud.gov/offices/adm/grants/nofa05/grpcoc.cfm).

2.8 What is the facility code in the "Program Identification Information" data element?

The Program Identification Information data element is composed of 4 different codes: a 10-digit FIPS code, a Continuum of Care code, a facility code, and a program type code. A facility code should be assigned to each facility where services provided and is locally determined. That is, every building where homeless services are provided should be assign a facility code, and CoCs have the discretion to choose how the facility code will appear in the HMIS. For example, a CoC with 50 facilities may choose to sequentially number the facility code from 01 to 50.

2.9 What type of service should be recorded as "Temporary housing and other financial aid" in the Services Received program-specific data element (3.9)?

The "Temporary housing and other financial aid" response category is intended to capture emergency financial assistance for housing-related expenses, such as rental assistance and security deposit. The response category was not meant to capture "temporary housing" (i.e., a shelter or transitional housing) as a service type.

2.10 Should programs collect the detailed information in the Veteran's Information data element (optional data element 3.16) for each military service era?

The Veteran's Information data element collects detailed information about a veteran's military experience, including his/her military service era, duration of active duty, service in a war zone, branch of the military, and discharge status. Programs collecting this information should allow clients to identify multiple service eras and branches of the military. However, it is not necessary to collect all of the detailed information (i.e., duration of active duty, service in a war zone, and discharge status) for each military service era. This information should be captured for the most recent service era.

3. Implementing the HMIS Notice: Privacy Standards

3.1 Can a HIPAA covered entity collect the required HMIS data elements and still be consistent with the HIPAA rule?

Yes. The HIPAA rule established a set of basic national privacy standards and fair information practices governing many health records. However, the HIPAA rule generally avoids telling covered entities what information they can and cannot collect.

The rule's "minimum necessary" standard sometimes limits a use, disclosure, or request of protected health information (PHI) by HIPAA covered entities. The only limitation on *collection* applies when a covered entity requests PHI *from another covered entity*. In that case, a requester must sometimes make reasonable efforts to limit the request to the minimum information necessary to accomplish the intended purpose of the request (45 C.F.R. §164.502(b)(1)). This provision is not a general limitation on the collection of information and does not restrict data collection from a data subject.

3.2 Do the HMIS privacy standards conflict with other federal laws regulating the collection and uses of personal information?

Federal laws regulate the collection, use, or disclosure of personal information in some circumstances. These laws include the American with Disabilities Act (ADA), Violence Against Women Act (VAWA), Victims of Crime Act (VOCA), and Drug and Alcohol Confidentiality statutes, as well as other federal privacy laws that typically regulate specific record keepers or specific records. State laws may also impose restrictions on the collection, use, or disclosure of personal information. Where another law requires additional confidentiality protections, the HMIS Notice yields to those protections. Put differently, there cannot be a conflict between the HMIS Notice and other laws where these laws require stricter confidentiality protections. An appropriate government entity (e.g., state attorney general) must determine whether the law provides stronger confidentiality provisions than the HMIS privacy standards.

A Covered Homeless Organization (CHO)[1] can comply with both the HMIS standards and other privacy laws, although there will be times when other laws with stricter confidentiality protections prevail over the HMIS standards. Whether any additional privacy laws are relevant to a homeless service provider will depend on what services are offered by the provider. For a CHO that offers federally funded drug/alcohol treatment services, the Drug and Alcohol Confidentiality statutes and regulations will normally prevail because they regulate disclosure more strictly than the HMIS standards. If a CHO provides e-mail facilities to clients, it may have to pay attention to the Electronic Communications Privacy Act before disclosing e-mail records. Few other federal privacy laws are likely to apply to CHOs. If a CHO engages in activities involving credit reports, banking, video tape rental, or federally funded educational activities, asking questions and doing more research about privacy laws is advisable.

In addition, questions may arise about research confidentiality laws. Research confidentiality laws could be relevant to a CHO that receives a research grant or contract with a "certificate of confidentiality" that limits the use or disclosure of personal information. "Certificates of confidentiality" or similar protections generally limit use and disclosure of personally identifiable information to the research or statistical purpose for which the information was obtained. Because of the narrow scope and effect of these certificates, they may not apply to a homeless service provider's operational files and are not likely to affect basic HMIS disclosures. However, the scope of each certificate must be reviewed to see if it is relevant.

[1] A CHO is defined in the final Notice as "any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS" (FR 4848-N-02, 45928).

3.3 What happens if other federal, state, or local laws are found to be in conflict with the HMIS privacy or security standards?

There are two important provisions in the HMIS Notice regarding possible conflicts between federal, state, or local laws and the HMIS privacy standards.

First, some providers of services for the homeless may be covered by the Health Insurance Portability and Accountability Act (HIPAA). The final notice states that any organization that is covered under the HIPAA (i.e., is designated as a HIPAA covered entity) is not required to comply with the privacy or security standards in the HMIS Notice if the provider determines that a substantial portion of its protected personal information is covered by HIPAA. Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules.

Second, the HMIS rule states expressly in section 4.2 that a Covered Homeless Organization "must also comply with federal, state and local laws that require additional confidentiality protections" (45929). The effect of this provision is that any stronger confidentiality provision in any other law remains in force and would supersede the HMIS standards. An appropriate government entity (e.g., state attorney general) must determined whether the law provides stronger confidentiality provisions than the HMIS privacy standards.

3.4 For a basic community shelter (CHO) with no federal funding, who holds the shelter accountable for the misuse of client information collected for HMIS purposes?

Accountability can come from many different sources. The HMIS privacy standards have an accountability component that requires a Covered Homeless Organization (CHO) to have a complaint procedure and to have staff sign a confidentiality agreement. Under the additional privacy protections described in the HMIS standards, a CHO may also conduct staff training in privacy, provide audits trails for regularly reviewing compliance with the privacy requirements, establish an appeal process for privacy complaints, or designate a chief privacy officer to supervise implementation and compliance with the privacy standards. These provisions mean that the first line of accountability is internal. A CHO has primary responsibility for complying with privacy standards.

A CHO may also be held accountable by its peers and by law. If a CHO violates privacy or other applicable rules, other organizations in the Continuum of Care may be affected and may change the way they interact with the CHO. Misuse of client information may also be a violation of federal or state criminal statutes. Other possible accountability measures include government investigations, civil enforcement actions, and private lawsuits.

3.5 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures required by law"?

The HMIS baseline standard allows a Covered Homeless Organization (CHO) to disclose protected personal information (PPI)[2] when required by law if the disclosure complies with, and is limited to, the

[2] Protected Personal Information is defined in the final Notice as "any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific

requirements of the law. That is, if a request for PPI is based on, and within the scope of, a specific legal requirement, the CHO may disclose the PPI without violating the HMIS standard. To qualify, the law must *require* (and not merely permit) the disclosure. The two examples below demonstrate how this provision may be applied.

Example 1: State law requires that all health care providers report to the police the name of any individual found to be suffering from a gunshot wound. A CHO providing health care discloses to police the name of an individual suffering from a gunshot wound. The disclosure is consistent with the HMIS standard. However, the disclosure must be limited to the legally mandated pieces of information. Disclosing age or Social Security Number, for example, would not be permissible under the standard unless the law requiring disclosure also requires disclosure of those elements.

Example 2: The local police ask for access to the CHO's client database to browse through it for names of persons the police are interested in locating. The police cite a section of the USA PATRIOT Act of 2001 (50 U.S.C. 1861) as authority for the request. The CHO refuses to make the disclosure, and the refusal is consistent with and required by the HMIS privacy standard. Section 215 of the USA PATRIOT Act allows the Director of the Federal Bureau of Investigation to seek a court order requiring the production of books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities. The authority of section 215 of the USA PATRIOT Act cannot be exercised either by local police or without a court order.

3.6 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures to avert a serious threat to health or safety"?

A Covered Homeless Organization (CHO) may disclose protected personal information if (a) the CHO, in good faith, believes the disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; *and* (b) the disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat. Disclosures under this authority may be made to law enforcement officials or to other persons if these conditions apply.

Example 1: An individual in a shelter threatens to harm another individual with a knife. The CHO calls the police and discloses the name of the individual. The disclosure is consistent with the standard because the threat to health or safety is serious and imminent and because the police may be able to prevent the threat.

---

individual; or (3) can be linked with other available information to identify a specific individual" (FR 4848-N-02, 45928).

Example 2: The police ask a CHO for the name and other information about an individual believed to have left the CHO's homeless shelter and who is now holding another individual hostage. The CHO discloses the name and Social Security Number of the individual. It declines to provide other information in its possession because it does not believe that the additional information would be helpful in preventing or lessening the threat. The disclosure of the name is consistent with the standard. The refusal to disclose other information is also consistent with the standard.

3.7 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures about victims of abuse, neglect, or domestic violence"?

A Covered Homeless Organization (CHO) may disclose protected personal information (PPI) about a victim of abuse, neglect, or domestic violence if:

(a) *required* by law;

(b) the victim agrees; *or*

(c) the disclosure is expressly *authorized* by law and the CHO believes the disclosure is necessary to prevent serious harm to the victim or other potential victims; *or* if the victim is unable to agree because of incapacity, the CHO believes that the law enforcement request for PPI is not intended to be used against the victim and that an immediate law enforcement activity that depends upon the disclosure would be considerably and adversely affected by waiting until the individual is able to agree to the disclosure.

With a few exceptions described in section 4.1.3 of the HMIS privacy standards, a CHO that makes a permitted disclosure about a victim of abuse, neglect or domestic violence must promptly inform the victim that a disclosure has been or will be made.

Example 1: A CHO discloses PPI to a law enforcement agency with the oral consent of the victim. The disclosure is consistent with the standard.

Example 2: The police ask for information about a victim of domestic violence under a specific statutory provision that authorizes disclosure of PPI to the police. The police orally assure the CHO that they do not intend to use the PPI against the victim. The police also represent that they have an immediate law enforcement need for the PPI that would be significantly affected by a delay to seek the consent of the individual. The CHO is unable to obtain consent because of the victim's incapacity. Because the statutory provision authorizes but does not require disclosure, the CHO declines to disclose the information, which is consistent with the standard. The CHO may choose to disclose the information, provided that the CHO informs the victim that the disclosure was made at the first opportunity.

3.8 In section 4.1.3 of the HMIS privacy standards, what do the standards mean by "uses and disclosures for law enforcement purposes"?

A Covered Homeless Organization (CHO) may disclose protected personal information (PPI) to a law enforcement official for a law enforcement purpose:

- if the disclosure is in response to a lawful *court order*, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

Example 1: The police arrive at the premises of a CHO with a legally sufficient search warrant authorizing the search and removal of records containing PPI. A CHO that allows the police to exercise the warrant does not violate the HMIS standard because a search warrant constitutes legally authority to seize records.

- if the law enforcement official makes a *written request* for protected personal information that: (1) is signed by a supervisory official of the law enforcement agency seeking the PPI; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; *and* (5) states that de-identified information could not be used to accomplish the purpose of the disclosure;

Example 2: A police officer brings a written request signed by a supervisory official asking for access to the CHO's client database to browse through it for names the police may be interested in. The CHO refuses the request. The refusal is required by the standard because the request is not specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought and because the request does not state that de-identified information could not be used to accomplish the purpose of the disclosures.

- if the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO;

Example 3: A client of a shelter assaults another client in the dining room of the shelter. The CHO calls the police and discloses the names of the individuals involved and the circumstances of the assault. The disclosure is consistent with the standard because the PPI disclosed is evidence of a crime that occurred on the premises of the CHO.

- if the disclosure is in response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics;

Example 4: A police officer asks a CHO for information to help in locating a suspect believed to be homeless. The CHO discloses information about the name, Social Security Number, and distinguishing physical characteristics of several clients. The disclosure is consistent with the standard.

- if (1) the official is an authorized *federal official* seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and (2) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

Example 5: The local police ask a CHO to disclose information about the location of named homeless clients for use in connection with a Presidential visit planned in the next week. The CHO refuses to disclose the PPI. The refusal is permitted by the standard because disclosures made in connection with the provision of protective services must be to an authorized *federal* official.

3.9 What is meant by client "consent" for all uses and disclosures specified in the HMIS privacy standards?

Consent can be an important element of information privacy. The HMIS privacy standards allow a Covered Homeless Organization (CHO) considerable discretion in deciding how to use consent to control the collection, use, and disclosure of personal information about clients. Under the baseline requirement in the HMIS Notice, a CHO can infer or assume that clients have consented to all processing activities described in its privacy notice. That means that oral or written consent is not necessary under the HMIS standards. A CHO could decide to seek oral or written consent before collecting, using, or disclosing personal information. The HMIS standards deliberately allow each CHO to select the most appropriate policy for its own operations. The standards require all CHOs to describe the policy in their privacy notices and to adhere to the policy. Each CHO has to strike the right balance for its clients and itself in the use of consent. Choices presented to clients should be fair, understandable, and meaningful. A CHO must be able to manage the choices it offers clients. Consent is not always practical or possible, especially when external obligations will not support individual choices.

3.10 Can HUD provide sample privacy notices that are compliant with the HMIS standard?

A sample privacy notice is attached to this FAQ (see Appendix A). The sample privacy notice meets the baseline requirements of the HMIS privacy standards. Each provider may need to add or adjust the information in this sample notice to reflect its own requirements. The notice includes instructions about making appropriate changes to the notice. It also identifies some optional elements that a provider may choose to include.

3.11 Who is obligated to post the notice of privacy practices on a website?

The obligation to post a privacy notice falls on a Covered Homeless Organization (CHO) that "maintains" a public web page. A CHO is any organization—including its employees, volunteers, affiliates, contractors, and associates—that records, uses or processes protected person information on homeless clients for an HMIS. The word "maintains" should be read as meaning "controls the content of a web page about the CHO." If a CHO does not have its own public web page, it has no obligation to post the notice on any other web site.

In some cases, a CHO is affiliated with a local, state, regional, or national organization (hereafter called an "organization"), and the obligation to post a privacy notice will vary depending on a few important considerations.

- If the organization maintains a separate web page for each local CHO and the CHO effectively controls the content of its own page, the privacy notice must be posted there. The point of the standard is that any CHO that describes its operations and activities on a web page should include its privacy notice. It does not matter if the organization, contractor, or other host technically maintains the web page.

- If the organization maintains a separate web page for each local CHO but the organization controls the content, then the CHO has no obligation to post its privacy notice because the local CHO does not control the content. Posting privacy notices would clearly be permissible and desirable, however.

- If the organization is itself a CHO, it must post its own privacy notice on any public website that it maintains. The organization does not have an obligation to post a privacy notice for an affiliated CHO. Any obligation to post falls directly on a CHO and does not migrate elsewhere based on ownership, control, affiliation, or other relationship.

- Finally, nothing prevents an organization from hosting privacy policies for local CHOs that do not have public web pages. A CHO can go beyond the requirement of the privacy standards by using an organization or any other contractor to host its privacy notice, even if no other information about the CHO is available on the web site.

4. Implementing the HMIS Notice: Technical Standards

4.1 Which of my computers and systems are affected by the new security standards?

All computers and systems that co-exist on the same trusted network as machines used to access HMIS are required to meet the baseline security standards. The security standards also apply to remote machines, such as home office computers, that can access the network via a Virtual Private Network (or VPN) on which HMIS workstations are housed.

4.2 Who is required to implement Public Key Infrastructure (PKI) or other similar means to restrict access to the HMIS?

Section 4.3.1 System Security: Public Access states: "HMIS that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means" (45931). This provision requires communities that use the Internet as a connecting network for transmitting or receiving HMIS data— a common architecture for web-based HMIS —to implement access controls in addition to the required use of usernames and passwords. This provision covers the majority of HMIS web/application servers that are currently in use.

The additional security measures described in Section 4.3.1 include any combination of PKI (digital certificates), VPN (Virtual Private Networks), Extranets, or limiting the range of Internet Protocol (IP) addresses that may communicate with the HMIS. This additional layer of security is critical to protecting personal information.

4.3 What is the definition of a "public forum"?

The public access provision of the security requirement mandates higher security requirements for an HMIS that uses a public forum, such as the Internet, to collect or report data. In determining whether this provision applies to your organization, the question to ask is: *Does **any** part of the HMIS system (including application/web servers) use the Internet to transmit or receive data?"* If the answer is yes, then the provision applies to the HMIS and either a Public Key Infrastructure (PKI) mechanism or restricted IP access is required to limit access to the components of the system which are public-facing (i.e., can receive requests from anywhere on the Internet). The security standards also allow communities to use a combination of PKI certificates and IP-limited access to restrict public access.

4.4 Are PKI implementations difficult and costly?

The resource demands of implementing PKI technologies to protect personally identifying information in an HMIS are roughly proportional to the size of the networks involved and the number of users accessing the system. A number of commercial and open source software packages are available to create and sign digital certificates, and installation onto browser workstations can be automated. Communities are encouraged to consider solutions as wide ranging as: full-service Certificate Authorities such as Verisign, Thawte, RSA, Equifax, and GTE (listed as default trusted Root Authorities in nearly all modern browsers); commercial applications like Microsoft Certificate Server; and the no-cost and open source OpenSSL toolkit.

Several large HMIS implementations have used these tools successfully to implement PKI, and there are a few resources available that describe these implementations:

- The City of Chicago: http://hmis.info/ta_resources_data.asp?topic_id=8
  (click on City of Chicago PKI strategy)

- The City of Seattle's Safe Harbor implementation of PKI:

http://www.safeharbors.org/Docs/PKICertificateSetupSteps%20v1.pdf
http://transact.wa.gov/
http://www.safeharbors.org/HMISFAQ.htm

HUD recognizes that it will take time to fully implement the Public Access security standard. HUD will continue to offer technical assistance to communities implementing HMIS, and to facilitate the exchange of implementation strategies across communities through HUD's website and HMIS.info.

4.5 Is PKI or encryption required for an HMIS using Citrix or Microsoft Terminal Services?

If the users' workstation accesses the Citrix or Terminal Services server over a public forum, then strong encryption (128-bit minimum) and some mechanism to limit access such as client-side PKI digital certificates or IP-based restrictions are required by the HMIS standards. Depending on the age of the system and the type of operating system on the workstations accessing Citrix, strong encryption may not be enabled by default and communities would need to manually enable the encryption. Many implementations of Citrix and Terminal services utilize 40-bit encryption, which does not meet the baseline security standards.

In addition, a minimum 128-bit encryption is needed for all information being exchanged with the server, i.e., not just the login exchange, but also the "data channels." That is, some configurations of remote access software only encrypt the initial login and password exchanged between the workstation and server, but the actual HMIS data being entered or queried is sent unencrypted. This type of configuration is inadequate to properly protect personally identifying information transmitted across the Internet. All "data channels" also require encryption.

4.6 When the final notice refers to an "individual firewall" for a workstation, what does that mean?

Section 4.3.1 System Security: Firewalls states: "Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall" (45931).

A firewall is defined as either software or hardware (or combination of both) that limits network traffic. Individual workstations that can access the Internet directly can meet the standard in a number of ways. In the case of a Microsoft Windows system, this could include the use of personal firewall software or even the built-in personal firewall. On other systems such as Mac OSX or Linux, the operating system typically includes similar Personal Firewall facilities via system configuration (or directly through iptables, ipchains, etc.). Alternatively, a hardware firewall (including a Small Office/Home Office (SOHO) cable/DSL router firewall) can also be used.

4.7 Can a "wireless network" (or connection) comply with the HMIS security standards?

Although not explicitly discussed in the HMIS Notice, communities that use wireless networks to access HMIS must address the important security issues associated with this technology by paying particular attention to the Public Access, Virus Protection, and Firewall provisions in the HMIS Notice (Section 4.3.1).

An HMIS that can be accessed via a wireless network will almost certainly require the use of PKI (digital certificates) or VPN (Virtual Private Networks), and limit the use of extranets (limited IP addresses) to non-wireless users. In addition, communities that use wireless networks must maintain current anti-virus software and use personal firewalls, and should consider using enhanced access controls and encryption technologies that exceed the baseline security standards in the HMIS Notice. For example, Wireless Protected Access (WPA) software provides strong data protection by using encryption, access controls, and user authentication that are designed specifically for a wireless system.

4.8 Is a firewall needed if we use Citrix to access our HMIS?

The use of Citrix, regardless of its configuration, does not exempt a community from using a firewall either at a perimeter network point or directly on the workstation itself, if the workstation has Internet connectivity. If the individual workstation that accesses Citrix uses a dial-up connection, then a local firewall is needed on that workstation.

5. HMIS Data Standards and HUD's Annual Progress Reports

5.1 Was there an error in the "Cross-walk of HMIS and APR Response Categories for Destination" on page 45919 of the final notice?

Yes. There is a coding error in the "Cross-walk of HMIS and APR Response Categories for Destination." The coding error was associated with HMIS response categories 15 (foster care home or foster care group home) and 16 (places not meant for human habitation).

A revised cross-walk is provided in Appendix B.

5.2 How do the new ethnicity and race categories in the final notice correspond to the categories in the Annual Progress Report?

The race and ethnicity categories in the final notice are required by the Office of Management and Budget (OMB). The HMIS standard response categories for ethnicity (Non-Hispanic/Non-Latino or Hispanic/Latino) are identical to the APR categories.

The five HMIS race categories are: American Indian or Alaska Native; Asian; Black or African American; Native Hawaiian or Other Pacific Islander; and White. Clients must be able to select multiple race categories. These ethnicity and race response categories can be combined to describe the characteristics of any homeless client.

The HMIS data standard and the APR response categories are identical where a client reports just one race. A problem arises when a client reports more than one race because the current APR lists only four possible combinations (for example – Asian and White) plus an "other multi-racial" category, while the HMIS allows for a much larger number of combinations. Where a client reports two or more races that are not specifically combined in the APR response categories, the client should be counted in the "other multi-racial category" for APR reporting purposes.

Appendix A:

Baseline Model Privacy Notice for Homeless Organizations

July 2005

How to Use This Model Privacy Notice

The Homeless Management Information System privacy standards require each covered homeless organization (CHO) to publish a privacy notice. The standards establish baseline privacy requirements for CHOs. The standards also include additional privacy protections that a CHO may adopt. CHOs must also comply with mandated security standards. The security standards are not addressed in this model notice.

This model notice assists a CHO that seeks to meet the baseline privacy requirements. The HMIS privacy standards allow each CHO to adopt additional privacy protections if it chooses. A separate optional model notice has language that a CHO can use to describe the additional privacy protections set out in the HMIS standards. The standards set out numerous additional privacy protections, and a CHO may also adopt other privacy protections not specifically suggested in the standards.

If a CHO is subject to federal, state, or local laws that require additional confidentiality protections, the CHO must comply with those laws. The HMIS standards do not exempt CHOs from other laws. In developing a privacy notice, each CHO should make appropriate adjustments required by another applicable law.

For a CHO using only the baseline elements, the language in this model notice will need some customization. Each organization must add or adjust the information in this notice to reflect its own requirements. Square brackets [like these] show where basic descriptive information, such as name and address, should be added to the model notice.

The notice also includes instructions about customizing the notice to reflect local policies and practices. Curly brackets **{like these}** contain directions to the drafter of the notice. They indicate where it is appropriate to include custom language or offer other advice. The verb used in the curly brackets tells you whether additional language is mandatory (e.g., add, include or make) or optional (e.g., consider adding). In a few instances, the model notice also identifies some optional elements that an organization may choose to include. A *customization box* like this contains these instructions and optional elements:

Customization Box: Box Title

{A box like this one contains more detailed instructions for customizing the notice to local requirements. It may also suggest optional elements or provide model language to include.}

Preparing a baseline privacy notice for your CHO using this model will require some effort. Find all the identified parts of the notice that require customization and provide the information as indicated. In a few instances, it will be necessary to write descriptions of your organization's information processing practices.

Think carefully about the contents of your privacy notice. A CHO is bound by the policies in its privacy notice. This means that each CHO may need to make administrative or procedural changes in its operations in order to implement the privacy standards that it adopts. Among other things, the notice requires that each staff member must receive and acknowledge receipt of a copy of this privacy notice.

An organization may find it appropriate to accomplish several purposes with its privacy notice. The notice informs clients about the organization's privacy practices. It may also include specific directions to the organization's staff about procedures and responsibilities. That is an option. Alternatively, an organization may choose to have a separate document to describe internal procedures and responsibilities.

A CHO has discretion in deciding how much detail to include in its privacy notice. In several places, the customization boxes direct CHOs to describe aspects of record keeping practices, such as the category of records maintained, sources of information, and routine sharing of records with affiliated organizations. The notice should contain as much detail as it is practicable to include consistent with the goal of fairly providing the reader of the notice with a reasonable understanding of what happens to personal information.

A Note About Uses and Disclosures

The model notice includes a standard list of permissible uses and disclosures common to covered homeless organizations. Organizations should include them in their privacy notices unless there is a specific justification to do otherwise. Most uses and disclosures on the list are permissive. A homeless organization can always refuse, on a case-by-case basis, to make a permissive use or disclosure listed in its privacy notice.

In principle, a CHO may decline even to reserve the option to make a use or disclosure from the standard list by not including the use or disclosure in its privacy notice. It would clearly be appropriate to do so, for example, if a state law prohibited a particular use or disclosure. A privacy notice should reflect other restrictions that apply to homeless organizations.

A homeless organization that does not include a use or disclosure in its privacy notice must generally obtain written client consent for the use or disclosure. For example, if a homeless organization receives funding contingent on reporting client information to the funder or other party, the organization will be in an impossible situation if it relies on client consent. When a client refuses consent, the organization will violate the conditions of its funding.

Relying on consent as an alternative to maintaining a complete and accurate description of uses and disclosures in a privacy notice can create problems. The privacy notice describes the information practices of an organization for the world as well as for clients. Consent has a place, but the consent

process can raise conflicts of interest between organization and clients. Explaining consent and managing client choice can be complex and resource-intensive.

It is important to remember that not all disclosures are permissive. Disclosures required by other laws must be made in accordance with the terms of those laws. The HMIS standards do not exempt homeless organizations from compliance with other laws. Disclosures for oversight of compliance with HMIS privacy and security standards are mandatory and cannot be avoided by omitting the authority from the privacy notice. A privacy policy that does not include all mandatory disclosures is incomplete and not in accordance with the standard.

Organizations should take note that the restrictive procedures in the standard list (e.g., for disclosures about victims of abuse, for academic research, or to law enforcement) must be complied with when making those uses or disclosures. Those procedures belong in every privacy notice. A disclosure may be permissive, but the procedures in the HMIS standard must be followed when making the disclosure. Organizations must describe other procedures required by law, and they may include additional procedures if desired. For example, an organization can decide that disclosures for research or for law enforcement require the approval of the organization's director.

Homeless organizations should make changes to the standard list of uses and disclosures only with caution and forethought. In most cases, it will be appropriate to reserve the right to make standard uses and disclosures. The actual decision about whether to make a use or disclosure of a particular record can be postponed until the need arises. If a CHO includes a use or disclosure in its privacy notice, the CHO will not diminish its ability to decline to make the use or disclosure later. However, broad restrictions in a privacy notice may turn out to be unduly limiting, can create problems for organizations, and may be unfair to clients.

Baseline Model Privacy Notice for Homeless Organizations

Customization Box: Notice Summary

{A CHO may add an optional summary to the front of the notice. A short and simply written summary will help clients and others understand the purpose and contents of the notice. Here is a sample brief summary for the baseline model notice:}

Brief Summary

[Effective Date]
[Optional Version Number]

This notice describes the privacy policy of the [Name of Homeless Agency]. We may amend this policy at any time. We collect personal information only when appropriate. We may use or disclose your information to provide you with services. We may also use or disclose it to comply with legal and other obligations. We assume that you agree to allow us to collect information and to use or disclose it as described in this notice. You can inspect personal information about you that we maintain. You can also ask us to correct inaccurate or incomplete information. You can ask us about our privacy policy or practices. We respond to questions and complaints. Read the full notice for more details. Anyone can have a copy of the full notice upon request.

Baseline Model Privacy Notice for Homeless Organizations

Full Notice

[Effective Date]
[Optional Version Number]

A. <u>What This Notice Covers</u>

1. This notice describes the privacy policy and practices of [Name of Homeless Organization]. Our main office is at [Address, email/web address, telephone.]
2. The policy and practices in this notice cover the processing of protected personal information for clients of [Name of Homeless Organization]. **{Consider adding an explanation as described in the Scope of Policy Customization Box.}**

> **Customization Box: Scope of Policy**
>
> **{Each CHO should identify the category of records covered by the notice by including a fair description of covered/uncovered programs or activities here. For example, explain if the policy does not cover personal information about a client that might otherwise appear to be covered or if another privacy policy (e.g., the HIPAA health privacy rule) applies to some records. Examples of a fair description include:**
>
> *** All personal information that we maintain is covered by the policy and practices described in this privacy notice.**
>
> *** All personal information that we maintain for our shelter program is covered by the policy and practices described in this privacy notice. Personal information that the medical clinic collects and maintains is covered by a different privacy policy.}**

3. Protected Personal information (PPI) is any information we maintain about a client that:
   a. allows identification of an individual directly or indirectly
   b. can be manipulated by a reasonably foreseeable method to identify a specific individual, **or**
   c. can be linked with other available information to identify a specific client. When this notice refers to personal information, it means PPI.
4. We adopted this policy because of standards for Homeless Management Information Systems issued by the Department of Housing and Urban Development. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
5. This notice tells our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.

6. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment. **{Consider adding amendment process information as described in the Notice Amendment Process Customization Box.}**

Customization Box: Notice Amendment Process

{If a CHO has a formal process for amending its privacy notice, it would be appropriate to describe it here. Elements might include the administrative process for adopting amendments or methods for public dissemination of amendments.}

7. We give a written copy of this privacy notice to any individual who asks.

{If appropriate, include statement from Web Site Notice Alternative Box.}

Customization Box: Website

{If an organization has a website, then it must put a copy of its privacy notice on the website. It should reference the availability of the notice like this:}

8. We maintain a copy of this policy on our website at <www.---.org>.

B. <u>How and Why We Collect Personal Information</u>

1. We collect personal information only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes: **{Include a list of purposes as described in the Collection Purposes Customization Box.}**

Customization Box: Collection Purposes

{Each privacy notice must describe the purposes for which a CHO collects personal information, whether from the client or from a third party. Use or modify these descriptions as appropriate:}

a. to provide or coordinate services to clients
b. to locate other programs that may be able to assist clients
c. for functions related to payment or reimbursement from others for services that we provide
d. to operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions
e. to comply with government reporting obligations
f. when required by law
g. **{identify any other known purposes}**.

2. We only use lawful and fair means to collect personal information.
3. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.
4. We may also get information about you from: **{Include description of sources as described in the Information Sources Customization Box.}**

Customization Box: Information Sources

{Each privacy notice must describe the routine sources of information about clients. The description should be as specific as reasonably practicable. Examples of source descriptions include:}

a. Individuals who are with you
b. Other private organizations that provide services (identify)
c. Government agencies (identify)
d. Telephone directories and other published sources
e. **{list other regular sources of information}.**

5. We post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign says:

   We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the need of homeless individuals. We only collect information that we consider to be appropriate.

C. <u>How We Use and Disclose Personal Information</u>

1. We use or disclose personal information for activities described in this part of the notice. We may or may not make any of these uses or disclosures with your information. We assume that you consent to the use or disclosure of your personal information for the purposes described here and for other uses and disclosures that we determine to be compatible with these uses or disclosures:

   a. to **provide or coordinate services** to individuals **{Consider including a description of routine sharing as described in the Information Sharing Customization Box.}**

   b. for functions related to **payment or reimbursement for services**

   c. to **carry out administrative functions** such as legal, audits, personnel, oversight, and management functions

   d. to **create de-identified (anonymous) information** that can be used for research and statistical purposes without identifying clients

Customization Box: Information Sharing

{When a CHO maintains PPI in a manner that involves routine sharing with other organizations via a computer network, joint operations, combined files, or in other ways, describe the scope of sharing and the names or types of organizations. Include a statement like this:

"We share client records with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information."**}**

e. **when required by law** to the extent that use or disclosure complies with and is limited to the requirements of the law

f. to **avert a serious threat to health or safety** if

(1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, **and**

(2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat

g. to **report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority** (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence

(1) under any of these circumstances:

(a) where the disclosure **is required** by law and the disclosure complies with and is limited to the requirements of the law

(b) if the individual agrees to the disclosure, **or**

(c) to the extent that the disclosure is **expressly authorized** by statute or regulation, **and**

(I) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, **or**

(II) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought **is not intended to be used against the individual** and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

and

(2) when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:

(a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, **or**

(b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse,

neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.

h. for **academic research purposes**

(1) conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

(a) by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated CHO program administrator (other than the individual conducting the research), **or**

(b) by an institution for use in a research project conducted under a written research agreement approved in writing by a designated CHO program administrator.

and

(2) any written research agreement:

(a) must establish rules and limitations for the processing and security of PPI in the course of the research

(b) must provide for the return or proper disposal of all PPI at the conclusion of the research

(c) must restrict additional use or disclosure of PPI, except where required by law

(d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, **and**

(e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

i. to a law enforcement official **for a law enforcement purpose** (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

(1) in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena

(2) if the law enforcement official makes a **written request** for PPI that:

(a) is signed by a supervisory official of the law enforcement agency seeking the PPI

(b) states that the information is relevant and material to a legitimate law enforcement investigation

(c) identifies the PPI sought

(d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, **and**

(e) states that de-identified information could not be used to accomplish the purpose of the disclosure.

(3) if we believe in good faith that the PPI constitutes **evidence of criminal conduct** that occurred on our premises

(4) in response to an oral request for the purpose of **identifying or locating a suspect, fugitive, material witness or missing person** and the PPI disclosed consists only of name, address,

date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, **or**

(5) if

(a) the official is an authorized federal official seeking PPI for the provision of **protective services to the President** or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), **and**

(b) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

and

j. to comply with **government reporting obligations** for homeless management information systems and for oversight of compliance with homeless management information system requirements.

{If appropriate, comply with instructions in Other Uses and Disclosures Customization Box.}

Customization Box: Other Uses and Disclosures

{Continue description of other anticipated uses or disclosures here:

k. include other uses and disclosures}.

2. Before we make any use or disclosure of your personal information that is not described here, we seek your consent first.

D. <u>How to Inspect and Correct Personal Information</u>

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, **{Include an explanation of access and correction procedures as described in the Access and Correction Customization Box.}**

Customization Box: Access and Correction

{Describe access/correction procedures. For example, a simple procedure may be for an individual to ask any staff member for access.}

4. We may deny your request for inspection or copying of personal information if:
   (a) the information was compiled in reasonable anticipation of litigation or comparable proceedings
   (b) the information is about another individual (other than a health care provider or homeless provider)
   (c) the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
   (d) disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial
6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. We are developing and implementing a plan to dispose of personal information not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

F. Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices. **{Include explanation as described in Complaint Procedures Customization Box.}**

Customization Box: Complaint Procedures

{Describe the complaint procedure, including how an individual can file a complaint, how the complaint will be processed, and when and how the individual who complained will receive a response. The procedure should be clear enough so that staff members know what they are supposed to do.}

2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

{Consider adding a change history section as described in the Optional Change History Customization Box.}

Customization Box: Optional Change History

{A CHO may choose to include a change history as part of its privacy notice. A change history might include elements like this:

G. Privacy Notice Change History

1. **Version 1.0. October 30, 2004. Initial Policy**
2. **Version 1.1. January 15, 2005. Revised access/correction procedure.}**

Appendix B: Cross-walk of HMIS and APR Response Categories for Destination

HMIS Data Element 3.10: Destination Response Categories	APR Question 14: Corresponding Response Categories
Destination = 1 Emergency shelter	n = Emergency shelter
Destination = 2 Transitional housing for homeless persons	i = Transitional housing for homeless persons
Subsidy Type = 3 S+C	d = Shelter Plus Care (S+C)
Destination = 3 Permanent housing for formerly homeless persons (such as SHP or SRO Mod Rehab) AND Subsidy Type NOT EQUAL to 3	f = Other subsidized house or apartment
Destination = 4 Psychiatric hospital or other psychiatric facility	k = Institution, psychiatric hospital
Destination = 5 Substance abuse treatment facility or detox center	l = Institution inpatient alcohol or other drug treatment facility
Destination = 6 Hospital (non-psychiatric)	q = Other
Destination = 7 Jail, prison or juvenile detention facility	m = Institution jail/prison
Subsidy Type = 1 Public housing	b = Public housing
Subsidy Type = 2 Section 8	c = Section 8
Subsidy Type = 4 HOME Program	e = HOME subsidized house or apartment
Destination = 10 Room, apartment, or house that you rent AND Tenure = 1 Permanent AND Subsidy Type = 6 Other housing subsidy	f = Other subsidized house or apartment
Destination = 10 Room apartment or house that you rent AND Subsidy Type = 0 None	a = Rental House or Apt (no subsidy)
Destination = 11 Apartment or house that you own	g = Homeownership
Destination = 12 or 13 Staying or living in a family member's or friend's room, apartment or house AND Tenure = 1 Permanent	h = Permanent: moved in with family or friends
Destination = 12 or 13 Staying or living in a family member's or friends room, apartment or house AND Tenure = 2 Temporary	j = Transitional: moved in with family or friends
Destination = 14 Hotel or motel paid for without emergency shelter voucher	q = Other (Please specify)
Destination = 15 Foster care home or foster care group home	q = Other (Please specify)
Destination = 16 Place not meant for human habitation	p = Places not meant for human habitation (e.g., street)
Destination = 17 Other OR 8 Don't Know OR 9 Refused AND Subsidy Type NOT EQUAL to 1, 2, 3, or 4	r = unknown
HUD is discouraging programs from using the "Other supportive housing" APR response category. Programs should report destinations to housing that are permanent or transitional in APR categories (a) through (h) or in categories (i) through (j), respectively. Destinations to emergency shelters should be reported in APR category (n).	o = Other supportive housing